

NMCI Public Key Infrastructure (PKI) User Guide



Update
Version 2.0
07/02/2003
NMCI.60092.01.UA0

Revision History

The Revision History table below lists in chronological order each minor revision of this document. A minor revision is defined as a set of changes affecting fewer than 30 percent of the pages in the document.

-1- Date	-2- Author	-3- Revision Number	-4- Change(s) Made	-5- Affected Page(s)

¹**Date:** date of the revision, listed on the cover page (format: MM/DD/YY)

²**Author:** person(s) responsible for revising the document (first and last name)

³**Revision Number:** version number, as listed on the cover page

⁴**Change(s) Made:** list of modifications (e.g., section added, exhibit revised, paragraph deleted, etc.)

⁵**Affected Page(s):** list of pages that were revised (e.g., 1, 2, 4-6, etc.)

Entries in the Revision History table are deleted when a document undergoes a major revision, called a document update. A document update is defined as a set of changes affecting more than 30 percent of the pages in the document. Document updates do not need to be listed in the Revision History table.

For more information about Navy Marine Corps Intranet (NMCI) documentation, contact the manager of the Document Management Team (Sandra Ward, 703-742-1164, ISFDOCSMailbox@eds.com).

Document Storage

The NMCI Information Strike Force (ISF) Operations Library assigns identification (ID) numbers for NMCI documents and stores the master editions. To contact the library, telephone or e-mail the ISF Operations Librarian (James R. Taylor, 703-742-1940, ISFOPSLibrary@eds.com).

Table of Contents

1	Introduction	1
2	What is a PKI certificate and How are they used within the NMCI environment?	2
3	How to Request a PKI Certificate	3
3.1	Customer Technical Representative (CTR)	3
3.2	NMCI Local Registry Authority (LRA)	3
3.3	NMCI Users	3
4	How to Download your PKI Certificate	4
4.1	PKI Certificate Download Instructions.....	4
5	Using Your PKI Certificate For NMCI Remote Access Service (RAS)	19
6	Using Your PKI Certificate For NMCI Outlook Web Access (OWA).....	20
7	Frequently Asked Questions (FAQS) About PKI	21
8	Contact Information and Other PKI Resources	22

1 INTRODUCTION

Welcome to the *NMCI Public Key Infrastructure (PKI) User Guide*. This guide provides information on the process to acquire and use a PKI certificate within the NMCI environment. PKI certificates are required for those users who have an NMCI laptop and those who wish to check their NMCI e-mail from a non-NMCI workstation through Outlook Web Access (OWA). This document will outline the following information and processes concerning PKI certificates:

- What is a PKI certificate and how are they used within the NMCI environment?
- How to request a PKI certificate
- How to download a PKI certificate from the Department of Defense web site
- Using your PKI certificate for NMCI Remote Access Service (RAS)
- Using your PKI certificate for NMCI Outlook Web Access (OWA)
- Frequently Asked Questions (FAQs) about PKI Certificates
- Contact Information and other PKI resources

2 What is a PKI certificate and How are they used within the NMCI environment?

A PKI certificate is an electronic “document” officially linking a user’s identity with his/her Public Key. The three types of PKI certificates are as follows:

- **Identity** – Used to digitally sign documents or electronic forms. Identity certificates are also used to authenticate (identify) the user to applications. At a minimum, each individual will obtain an identity certificate.
- **Email Signature** – Used to digitally sign e-mail messages. Email Signature certificates are required only if an organization is using a PKI-enabled e-mail application.
- **Email Encryption** – Used to digitally encrypt e-mail messages. Email Encryption certificates are required only if an organization is using a PKI-enabled e-mail application.

***Note:** This document outlines instructions for obtaining an identity PKI certificate for use with the Remote Access Service (RAS) for NMCI laptop users and for Outlook Web Access. Email Signature and Email Encryption certificates can be stored on the Common Access Card (CAC). For more information about CAC Badges, visit the “User Information” section on the “Services” tab of the NMCI Homeport or <http://www.nmci-isf.com/userinfo.htm>.*

The identity PKI certificate authenticates a user’s identity to the NMCI environment thus allowing access to the NMCI network remotely through use of an NMCI laptop or through Outlook Web Access. By logging into your PKI certificate, authentication to access the NMCI network is granted. Without this authentication, laptop users will be unable to successfully access their NMCI Outlook e-mail and network drives.

Identity PKI certificates are considered “soft certificates” or certificates downloaded from the Department of Defense (DoD) website and stored on a floppy disk, not the user’s Common Access Card (CAC). For NMCI laptop users, the identity PKI certificate must be copied from the floppy disk onto the hard drive of the laptop. For users who wish to utilize Outlook Web Access (OWA) to check their NMCI e-mail from a non-NMCI computer, the certificate is loaded off the floppy disk and onto the Internet browser of the workstation.

3 How to Request a PKI Certificate

To obtain a PKI certificate, the IT Point of Contact (IT POC) or Customer Technical Representative (CTR) must grant approval for a command or location. The information below outlines the responsibilities of each individual with respect to the issuance of PKI certificates under NMCI.

3.1 CUSTOMER TECHNICAL REPRESENTATIVE (CTR)

Responsibilities: The CTR determines those users who will receive a PKI certificate. All NMCI laptop users must have a PKI certificate to remotely dial into the NMCI. For those users who wish to check their NMCI e-mail from a non-NMCI workstation, the CTR, at their discretion or the discretion of the Commanding Officer, will determine and submit the names of those users (in addition to NMCI laptop users) to the NMCI Local Registry Authority (LRA).

3.2 NMCI LOCAL REGISTRY AUTHORITY (LRA)

Responsibilities: The NMCI LRA for a location is responsible for generating PKI certificates for users identified by the CTR or Commanding Officer. Upon creation of the certificate, the LRA will print out a Certificate Registration Instruction Sheet (CRI) for each user. The LRA or Trusted Agent (an individual within the command authorized by the LRA to issue PKI certificates to users) will then meet with each user to distribute the CRI.

3.3 NMCI USERS

Responsibilities: Users need to meet with the LRA or a Trusted Agent. Since PKI certificates involve security privileges, users must present two forms of government issued identification and sign for the Certificate Registration Instruction Sheet (CRI) from the LRA or Trusted Agent. The CRI contains the “User Number” and “Access Code” allowing each user access to and permission to download their PKI certificate. Once the user has the CRI, they can download the PKI certificate following the instructions outlined below or on the *PKI Certificate Download Quick Reference Guide* available at <http://www.nmci-isf.com/userinfo.htm> or under the “User Information” section of the “Services” tab of the NMCI Homeport.

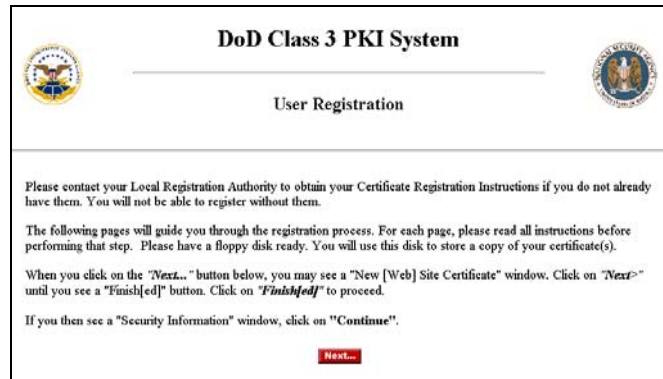
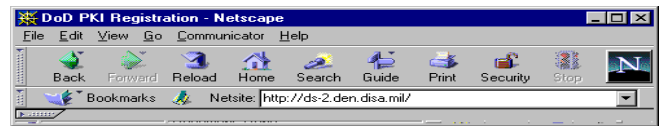
4 HOW TO DOWNLOAD YOUR PKI CERTIFICATE




This section describes the procedure for downloading your PKI certificate.



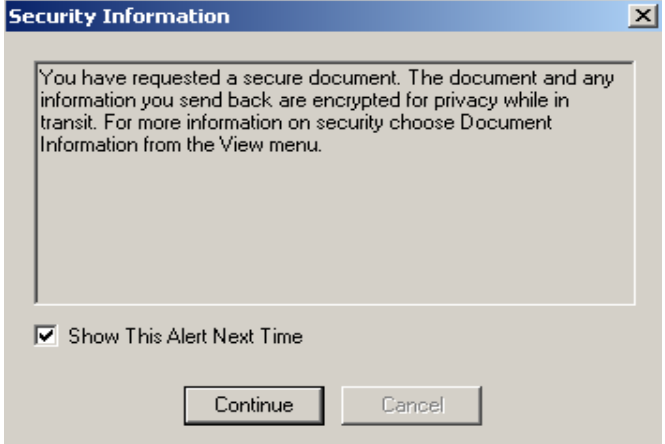
4.1 PKI CERTIFICATE DOWNLOAD INSTRUCTIONS

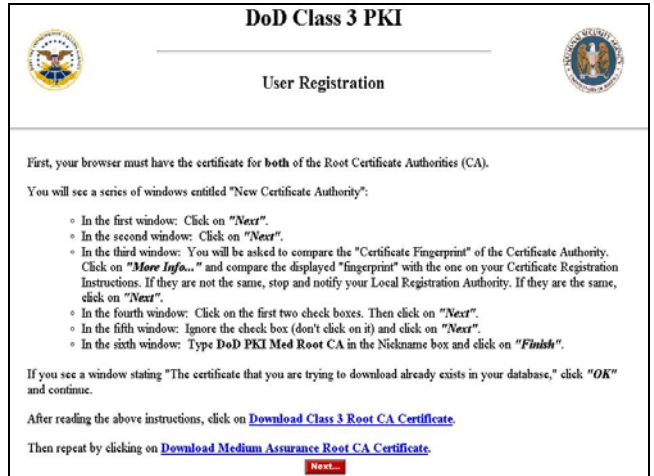


It is important to use Netscape Navigator browser to download your certificate. **Do NOT use Internet Explorer.**


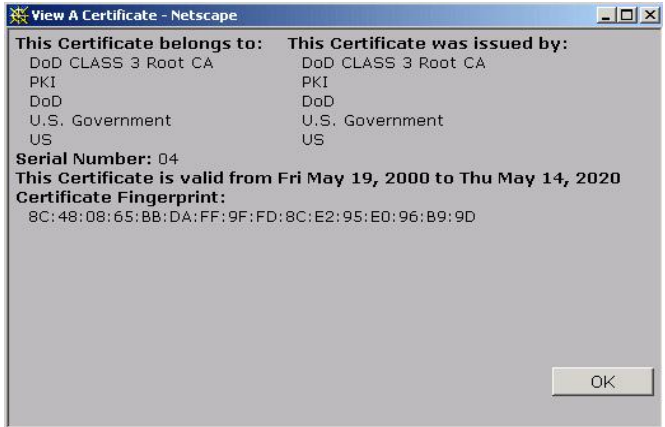

Procedures	
1.	<p>Open Netscape and access the Department of Defense (DoD) Public Key Infrastructure (PKI) homepage using either of the following addresses:</p> <p>http://reg.c3pki.chamb.disa.mil</p> <p>or</p> <p>http://reg.c3pki.den.disa.mil</p> <p><i>Note: It is recommended to access these sites during the morning hours due to high volume of users during the afternoon.</i></p>
2.	<p>Within the DoD Class 3 PKI System User Registration page, review the information and click Next.</p> <p><i>Note: Depending on which certificates are installed on your machine, you may not see steps 3-6. If you do not see these screens skip to Step 7.</i></p>



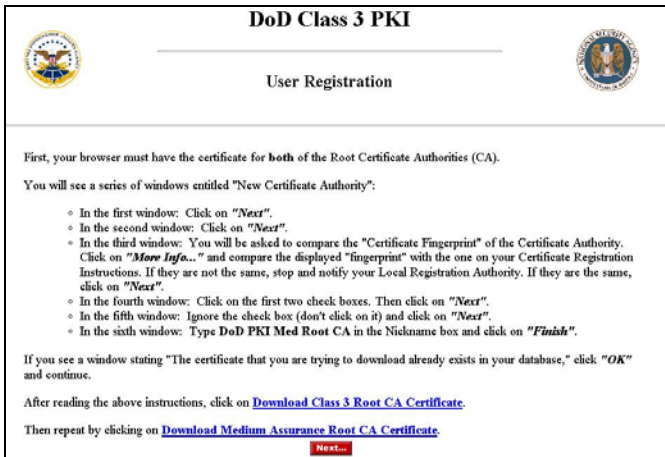





Procedures	
3.	<p>A window will appear. Read the information and click Next.</p> 
4.	<p>Read the information on this screen and click Next.</p> <p><i>Note: You may have to scroll down in the left frame menu to see this link.</i></p> 
5.	<p>Review the information displayed within the screen, select Accept this certificate for this session, and click Next.</p> 

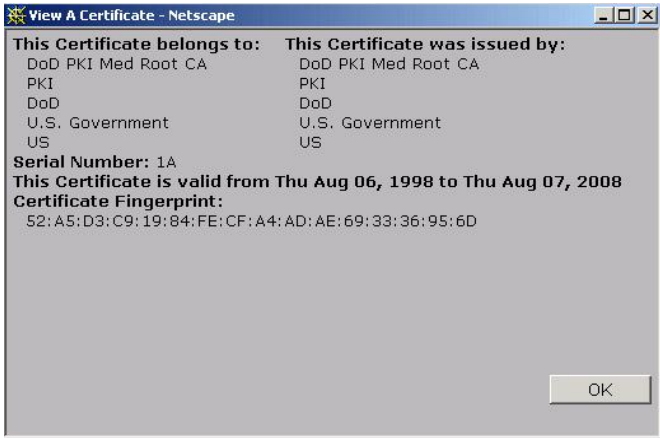


Procedures	
6.	<p>Within the following screen, ensure the Warn me before I send information to this site box is <u>NOT CHECKED</u> and click Next.</p> 
7.	<p>On the window indicating “You have finished examining the certificate presented by...” click Finish.</p> 
8.	<p>The Security Information window appears. Ensure the Show this Alert Next Time box is checked and click Continue.</p> 


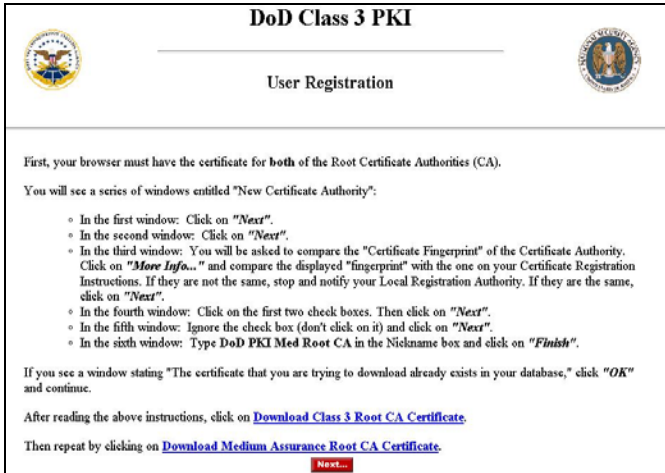
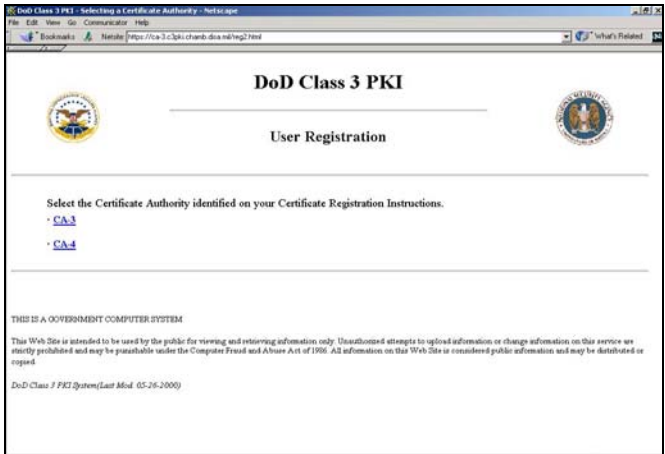
Procedures	
9.	<p>The DoD Class 3 PKI User Registration screen appears. Click the Download Class 3 Root CA Certificate link.</p> <p><i>Note: If you get a message that this certificate has already been installed proceed to Step 17.</i></p>
	 <p>The screenshot shows the 'DoD Class 3 PKI User Registration' page. It includes instructions for installing the certificate, such as clicking 'Next' in the first window, comparing fingerprints in the third, and clicking 'Finish' in the sixth. It also provides links to download the Class 3 Root CA Certificate and the Medium Assurance Root CA Certificate.</p>
10.	<p>Review the information and click Next.</p>
	 <p>The screenshot shows a Netscape dialog box titled 'New Certificate Authority'. It explains that accepting the authority has serious implications for security and asks the user to decide whether to accept it. The 'Next>' button is highlighted.</p>
11.	<p>Review the information and click Next.</p>
	 <p>The screenshot shows the same Netscape dialog box as in step 10, but with the '<Back', 'Next>', and 'Cancel' buttons visible at the bottom. The 'Next>' button is highlighted.</p>

Procedures	
12.	<p>Review the information within the following window and click More Info.</p> 
13.	<p>Compare the Certificate Fingerprint with the fingerprint on your Certificate Registration Instruction Sheet (CRI). If they differ, contact your LRA or Trusted Agent. If they are the same, click OK and then Next.</p> 
14.	<p>Within the displayed window, check all three boxes and click Next.</p> 

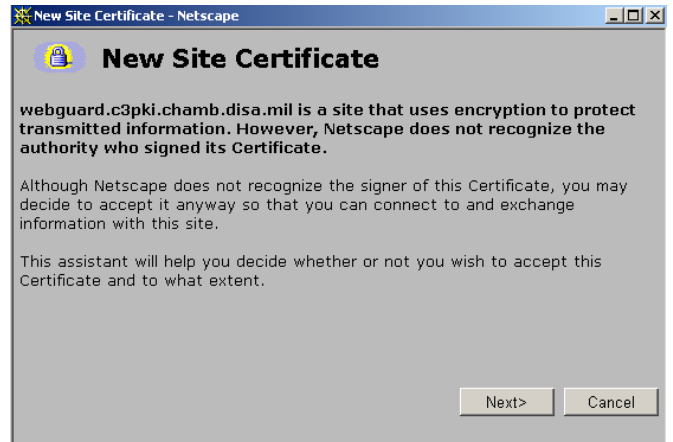
Procedures	
15.	<p>Within the displayed window, DO NOT check the box entitled Warn me before sending information to site certified by this Certificate Authority and click Next.</p> 
16.	<p>Within the displayed window, type DOD PKI Class 3 Root and click Finish.</p> 
17.	<p>The DoD Class 3 PKI User Registration page will appear. Click Download Medium Assurance Root CA Certificate.</p> <p><i>Note: If you receive a message indicating this certificate has already been installed, proceed to Step 25.</i></p> 


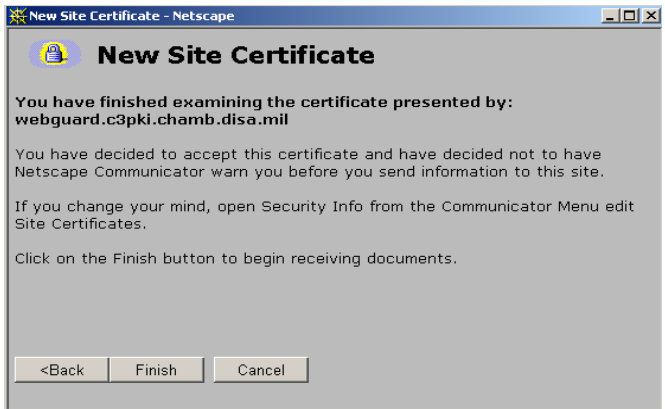
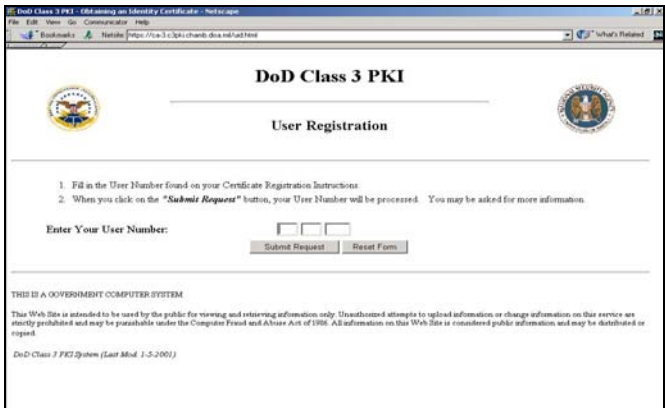
Procedures	
18. Review the information on the next two windows and click Next .	
19. Click Next .	
20. Review the information within the following window and click More Info .	

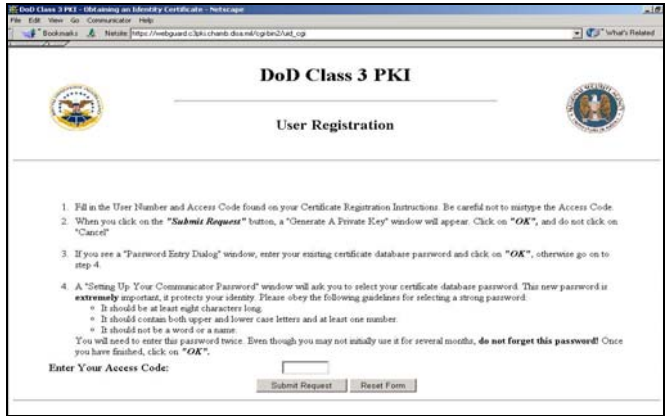

Procedures													
21.	<p>Compare the Certificate Fingerprint with the fingerprint on your Certificate Registration Instruction Sheet (CRI). If they differ, contact your LRA or Trusted Agent. If they are the same, click OK and then Next.</p>  <p>The dialog box titled "View A Certificate - Netscape" displays the following information:</p> <table border="1"> <thead> <tr> <th>This Certificate belongs to:</th><th>This Certificate was issued by:</th></tr> </thead> <tbody> <tr> <td>DoD PKI Med Root CA</td><td>DoD PKI Med Root CA</td></tr> <tr> <td>PKI</td><td>PKI</td></tr> <tr> <td>DoD</td><td>DoD</td></tr> <tr> <td>U.S. Government</td><td>U.S. Government</td></tr> <tr> <td>US</td><td>US</td></tr> </tbody> </table> <p>Serial Number: 1A This Certificate is valid from Thu Aug 06, 1998 to Thu Aug 07, 2008 Certificate Fingerprint: 52:A5:D3:C9:19:84:FE:CF:A4:AD:AE:69:33:36:95:6D</p> <p>OK</p>	This Certificate belongs to:	This Certificate was issued by:	DoD PKI Med Root CA	DoD PKI Med Root CA	PKI	PKI	DoD	DoD	U.S. Government	U.S. Government	US	US
This Certificate belongs to:	This Certificate was issued by:												
DoD PKI Med Root CA	DoD PKI Med Root CA												
PKI	PKI												
DoD	DoD												
U.S. Government	U.S. Government												
US	US												
22.	<p>Within the displayed window, check all three boxes and click Next.</p>  <p>The dialog box titled "New Certificate Authority - Netscape" contains the following text and options:</p> <p>Are you willing to accept this Certificate Authority for the purposes of certifying other internet sites, email users, or software developers?</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Accept this Certificate Authority for Certifying network sites <input checked="" type="checkbox"/> Accept this Certificate Authority for Certifying e-mail users <input checked="" type="checkbox"/> Accept this Certificate Authority for Certifying software developers <p><Back Next> Cancel</p>												
23.	<p>Within the displayed window, <u>DO NOT</u> check the box entitled Warn me before sending information to site certified by this Certificate Authority and click Next.</p>  <p>The dialog box titled "New Certificate Authority - Netscape" contains the following text and options:</p> <p>By accepting this Certificate Authority, you have told Netscape Communicator to connect to to connect to and receive information from any site that it certifies without warning you or prompting you.</p> <p>Netscape Communicator can, however, warn you before you send information to such a site.</p> <p><input type="checkbox"/> Warn me before sending information to sites certified by this Certificate Authority</p> <p><Back Next> Cancel</p>												

Procedures	
24.	<p>Within the displayed window, type DOD PKI Med Assurance and click Finish.</p> 
25.	<p>The DoD Class 3 PKI User Registration page will appear. Click Next.</p> 
26.	<p>On the displayed window, click the CA indicated on your CRI form.</p> 

Procedures	
27.	<p>Note: During the afternoon hours due to high volume of users, you may see additional screens, which are outlined in steps 27 through 31. If you do not see the screen displayed at the right, proceed to Step 32.</p> <p>If the screen to the right is displayed, click Next.</p>
28.	<p>Click Next.</p>
29.	<p>Review the information within the displayed screen, select Accept this certificate for this session, and click Next.</p>



Procedures	
30.	<p>Within the following screen, ensure the Warn me before I send information to this site box is <u>NOT CHECKED</u> and click Next.</p> 
31.	<p>On the window indicating “You have finished examining the certificate presented by...”, click Finish.</p> 
32.	<p>The DoD Class 3 PKI User Registration page appears. Enter the User Number from your CRI, and click Submit Request.</p> 

Procedures	
33.	<p>Within the following screen, enter the Access Code from your CRI, and click Submit Request.</p> 
34.	<p>The Generate A Private Key screen appears. Click OK.</p> <p><i>Note: If a password is already configured, you will go directly to the screen displayed in Step 37.</i></p> 

Procedures

35. Within the **Setting Up Your Communicator Password** screen, create a password for your PKI certificate and enter it in twice. Your PKI password must meet the following requirements:

- The password must be at least eight characters.
- It must contain both upper and lower case letters and at least one number.
- The password should not be a word or name.
- Do not use your NMCI network password.
- This password is valid for 3 years.

***Note:** The next window that appears will notify you the Certificate Request is being generated. Please wait for this screen to close. When this window disappears, your certificate has been successfully acquired.*



36. The **DoD Class 3 PKI System User Registration** page will display. Please review this information.

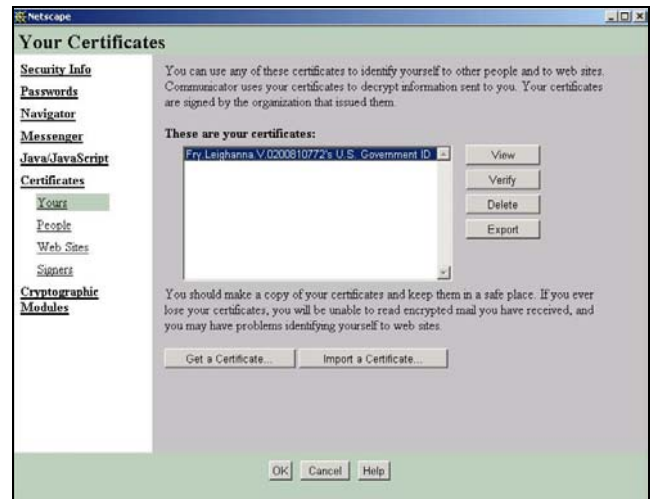


Procedures

37. Within the Netscape window, click the **Security** button in the Netscape toolbar. The second screen displayed on the right will appear. Click on **Yours** under the **Certificates** heading.


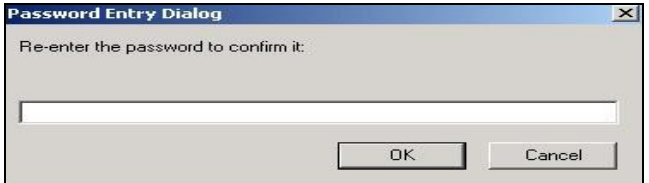
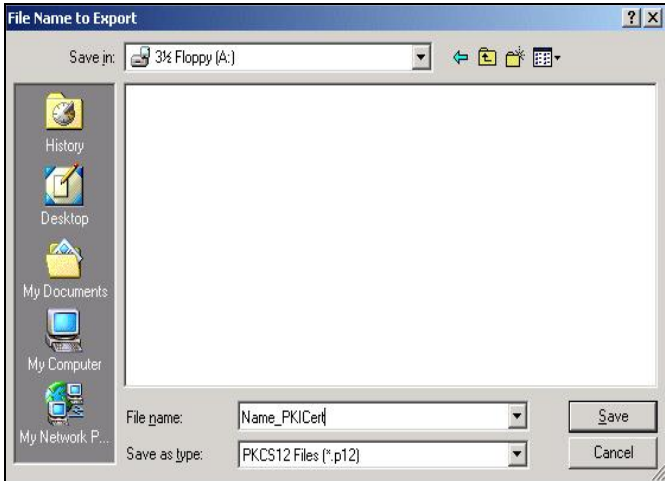



38. Under the window entitled **These are your certificates**, highlight your certificate and click **Export**.



39. Within the following screens, you will be asked to enter in a password.
Enter the password you created for your PKI certificate and click **OK**.



Procedures	
40. Enter the password you created for your PKI certificate and click OK .	
41. Enter the password you created for your PKI certificate and click OK .	
42. Insert a floppy disk into your computer. <i>Note: This floppy disk should be blank and should only contain your PKI certificate.</i>	
43. Select the 3 1/2-inch floppy or A: Drive from the Save in: drop down list. Enter a name (e.g., JSmith_PKIcert) for your certificate in the File name field. Click Save .	
44. A confirmation message window appears indicating you have exported your PKI certificate to the floppy disk. Click OK .	
45. Click Cancel to close the Your Certificates window within Netscape.	
46. Close your Netscape Browser window.	

5 USING YOUR PKI CERTIFICATE FOR NMCI REMOTE ACCESS SERVICE (RAS)

For NMCI laptop users, a PKI certificate is needed to allow access to the NMCI network when working remotely. A copy of your PKI certificate must be stored on the hard drive of your laptop so you can log into your certificate and authenticate your identity to the NMCI network. By authenticating your identity to the NMCI network through your PKI certificate, you can access your NMCI e-mail account and your network drives. To load your PKI certificate onto the hard drive of your workstation complete the following steps:

***Note:** The instructions below are associated with a new version of the Virtual Private Network (VPN) software called Alcatel used with your PKI certificate. You may have the previous version this VPN software called Timestep on your workstation. If you have not received the new Alcatel software, this update will occur shortly. The instructions apply for both versions of the software.*

1. Insert your floppy disk containing your PKI certificate into the floppy drive of your workstation.
2. Browse the floppy disk drive, highlight your certificate by right clicking on it, and select **Copy** from the menu that appears.
3. Locate the Certs folder on your NMCI workstation through the following path:

C:\Program Files\Alcatel\Certs

***Note:** If your workstation has the Timestep application installed instead of Alcatel, locate the certs folder through the following path:*

C:\Program Files\Timestep\Certs

***Note:** If you do not have a Certs folder, create one yourself and proceed to the next step.*

4. Open the Certs folder and select **Paste**. This will place a copy of your PKI certificate into that folder on your hard drive.

If you require assistance on locating the Cert folder or copying the PKI certificate into that folder, please contact the NMCI Help Desk at 1-866-THE-NMCI or 1-866- 843-6624. For instructions on how to use the NMCI Remote Access Service (RAS) with your NMCI laptop review the RAS portion of the “User Information” section available on the “Services” tab of the NMCI Homeport or visit www.nmci-isf.com/userinfo.htm.

6 USING YOUR PKI CERTIFICATE FOR NMCI OUTLOOK WEB ACCESS (OWA)

PKI certificates are also needed if you wish to access your NMCI e-mail account from a non-NMCI workstation (such as your home computer). Outlook Web Access (OWA) will allow you to read and send Outlook e-mail from a non-NMCI workstation. Users of OWA need to carry their PKI certificate on a 3.5-inch floppy disk to load into the Internet browser of the non-NMCI workstation. Instructions on how to load your PKI from your disk to a non-NMCI workstation are available on the “User Information” section available on the “Services” tab of the NMCI Homeport or visit www.nmci-isf.com/userinfo.htm to access the “Outlook Web Access” section.

7 FREQUENTLY ASKED QUESTIONS (FAQS) ABOUT PKI

The following questions outline some important reminders about your PKI certificate.

What if I already have a PKI certificate?

If you have had a PKI certificate issued to you before the NMCI transition process, please contact the NMCI Local Registry Authority (LRA) to validate your status. The LRA will provide you with additional information surrounding the issuance or re-issuance of a PKI certificate.

What if I lose my PKI certificate?

Since your PKI certificate is secure document assigned to you, it needs to be handled properly. If you lose your PKI certificate or if your PKI password becomes compromised, contact the PKI Help Desk at 1-800-582-4764, your NMCI LRA, or your Customer Technical Representative (CTR) immediately. The certificate will be revoked and a new certificate will be issued.

How long is a PKI certificate valid?

Your PKI certificate is valid for 3 years. Additionally, the password you assign to your certificate will not expire.

What if I forget my PKI password?

If you forget your PKI password, the certificate will need to be revoked and a new certificate will be issued.

Can I make a copy of my PKI certificate onto another floppy disk?

Although not recommended for security reasons, additional copies of your certificate can be placed onto additional floppy disks or to a CD.

8 Contact Information and Other PKI Resources

The following resources are available if you have additional questions about PKI certificates.

- For a listing of the NMCI Local Registry Authorities (LRAs) visit the “User Information” section of the “Services” tab of the NMCI Homeport or access www.nmci-isf.com/userinfo.htm and review the PKI/CAC section.
- Contact the PKI Help Desk: 1-800-582-4764 (located in Chambersburg, PA, available 24 hrs a day, 7 days a week)
- Contact the NMCI Help Desk: 1-866-THE-NMCI (1-866-843-6624)